CLAIMS

What is claimed is:

1. An apparatus, comprising:

an one-time programmable (OTP) memory including a plurality of memory cells, the plurality of memory cells being programmed to a default state or a state opposite the default state; and

a tamper detection circuit to sense when memory cell of the plurality of memory cells is programmed to the state opposite the default state.

2. The apparatus of claim 1, wherein each memory cell of the plurality of memory cells is adapted with fuse logic.

3. The apparatus of claim 2, wherein each memory cell of the plurality of memory cells is permanently programmed to the state opposite the default state by activating the fuse logic, and storing a data bit having a logical zero value.

4. The apparatus of claim 1, wherein each memory cell of the plurality of memory cells is adapted with anti-fuse logic.

5. The apparatus of claim 4, wherein each memory cell of the plurality of memory cells is permanently programmed to the state opposite the default state by activating the anti-fuse logic, and storing a data bit having a logical one value.

6. The apparatus of claim 1, wherein the tamper detection circuit includes combinatorial logic.

7. The apparatus of claim 6, wherein the combinatorial logic includes a plurality of NAND logical gates each coupled to one of the plurality of memory cells and a NAND gate having a plurality of inputs coupled to an output of each of the plurality of NAND logical gates.

8. The apparatus of claim 1, wherein the tamper detection circuit includes a Cyclic Redundancy Check (CRC) generator to compute a CRC value for data bits stored within the plurality of memory cells and a comparator to compare the CRC value to a pre-stored CRC value.

9. The apparatus of claim 8, wherein the pre-stored CRC value is a CRC value computed for the data bits stored within the plurality of memory cells at initial power-on of the apparatus and is stored in a memory separate from the OTP memory.

10. The apparatus of claim 1 being a processor that comprises the memory and the tamper detection circuit internally positioned within a semiconductor package of the processor.

11. An apparatus comprising:

an one-time programmable (OTP) memory including a plurality of memory cells, the plurality of memory cells programmed to either a default state or a state opposite the default state; and a tamper detection circuit to sense when all of the plurality of memory cells are programmed to the state opposite the default state.

12. The apparatus of claim 11, wherein each memory cell of the plurality of memory cells is adapted with fuse logic and is permanently programmed to a logical zero value, being the state opposite the default state, by activating the fuse logic.

13. The apparatus of claim 11, wherein each memory cell of the plurality of memory cells is adapted with anti-fuse logic and is permanently programmed to a logical one value, being the state opposite the default state, by activating the anti-fuse logic. .

14. The apparatus of claim 11, wherein the tamper detection circuit includes combinatorial logic.

15. The apparatus of claim 14, wherein the combinatorial logic includes a plurality of NAND logical gates each coupled to one of the plurality of memory cells and a NAND gate having a plurality of inputs coupled to an output of each of the plurality of NAND logical gates.

16. The apparatus of claim 11, wherein the tamper detection circuit includes a Cyclic Redundancy Check (CRC) generator to compute a CRC value for data bits stored within the plurality of memory cells and a comparator to compare the CRC value to a pre-stored CRC value.

17. A method comprising:

programming each of a first plurality of memory cells of an one-time programmable (OTP) memory to store data having an original bit value, the data being a series of data bits each having either a default state or a state opposite the default state and including at least one data bit having the default state and at least one data bit having the state opposite the default state;

determining whether all of the first plurality of memory cells are programmed to the state opposite the default state; and

disabling incoming encoded content from being decoded using the data from the OTP memory.

18. The method of claim 17 further comprising:

issuing a warning to be perceived by the user.

19. The method of claim 17 further comprising:

accessing a second plurality of memory cells previously loaded with the data with the original bit value; and

preventing access to the first plurality of memory cells.

20. The method of claim 19, wherein preventing access to the first plurality of memory cells comprises:

performing a logical operation on a stored value of the first plurality of memory cells and a value associated with a mask register; and

preventing access if a value produced by the logical operation is directed to an address different from an address associated with the first plurality of memory cells.